Department of Homeland Security Daily Open Source Infrastructure Report for 01 June 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Middletown Press reports three tools with low−levels of radiation were found in a Connecticut Yankee Nuclear Power Plant worker's pick−up truck −− which had previously left the site with the tools inside on Thursday, May 18. (See item 1)
- ABC reports Union Pacific Railroad officials say that a computer holding social security numbers and birth dates on approximately 30,000 employees has been stolen from the home of a employee in Omaha, Nebraska. (See item 12)
- Reuters reports the United States has tightened security with Canada in its northeast corner, and travelers from Canada are being required to show identification and submit to background checks at U.S. border posts in Vermont, New Hampshire, and Maine. (See item 18)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *May 31, Middletown Press (CT)* — **Contaminated tools leave Connecticut Yankee Nuclear site.** Three tools with low−levels of radiation were found in a worker's pick−up truck at the Connecticut Yankee Nuclear Power Plant site on Thursday, May 18. Further investigation determined that the truck had previously left the site with the tools inside, according to the

Nuclear Regulatory Commission (NRC). The tools in question were a mallet and two wrenches. The NRC received notification of the incident on Wednesday. State police and the state Department of Environmental Protection were also notified. "They really had a breakdown in their procedures and that's something we want to look at," said Neil Sheehan, NRC spokesperson. The Connecticut Yankee spokesperson, Kelley Smith, said it appeared that the equipment was inadvertently brought to the truck. No health or safety issues were apparent. The truck was searched after a radiation technician observed the worker hand a plastic gasket to another worker who was outside the radiological controlled area. The investigation, Smith said, was triggered when the gasket passed beyond the boundary of the two−acre area without being tested for radiation.
Source: http://www.middletownpress.com/site/news.cfm?newsid=16714918&BRD=1645&PAG=461&dept_id=10856&rfi=6

2. *May 30, KYW 1060 (PA)* — **Sunoco's siren warning system sounds off.** On Saturday, June 3, a new siren system will be tested around the Sunoco Refinery in South and Southwest Philadelphia, PA. The ten, 50−foot high sirens will be employed during an emergency. The sirens were installed because of a lawsuit filed by neighborhood organizers in the 1990's, following the release of an oil−tainted dust cloud from Sunoco's South Philadelphia refinery. Resident Al Caporali said, "I'm glad this system was installed, if there should be an accident or even a terrorist attack." John McCann of Sunoco said, "They can be heard at about 127−decibels at the base of the siren. They can be heard at 80−decibels a little more than a half mile away." The system will be tested the first Saturday of each month at noon, for 30 seconds.
Source: http://www.kyw1060.com/pages/40348.php

3. *May 30, Reuters* — **Florida utility prepares for major hurricanes.** Earlier this month the Florida Public Service Commission concluded that Florida Power & Light had not done enough to limit hurricane damage to the power grid following Hurricane Wilma in 2005. Up to 6.5 million people were left without lights, air conditioning, or hot water. FPL has instituted a five−point plan dubbed "Storm Secure," to take major steps to strengthen its transmission and distribution system and make it better able to withstand hurricane−force winds, said Geisha Williams, FPL's vice president of distribution. She said Storm Secure, launched on January 30, was only just getting under way, however. And while FPL has improved its reliability by about 50 percent since 1997, Williams acknowledged it still has a long way to go. "It won't be overnight; it's going to take a long time," said Williams, referring to a key goal of "hardening" the electric grid to withstand wind gusts up to 150 mph.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/30/AR2006053000352_pf.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *May 31, WCPO (OH)* — **Tanker explosion prompts bridge closure, building evacuation.** A BP tanker truck carrying gasoline and diesel exploded near the Roebling Suspension Bridge in Covington, OH, Wednesday morning, May 31. Surrounding buildings within a 1,000 feet radius were evacuated and the Roebling Suspension Bridge was closed. In addition, a nearby courthouse cancelled its docket for Wednesday.

Source: http://www.wcpo.com/news/2006/local/05/31/tanker.html

5. *May 30, WHEC−TV (NY)* — **Residents urged to remain indoors following ammonia leak.** Oakfield, NY, firefighters and Genesee County Emergency Services were called to the Birds Eye Frozen Food Plant Tuesday night, May 30, after a neighbor reported a strong odor. It turned out to be an ammonia leak. Residents near the plant were instructed to remain indoors, close their windows and turn off their air conditioners.
Source: http://www.10nbc.com/news.asp?template=item&story_id=19055

[Return to top]

Defense Industrial Base Sector

6. *May 31, InsideDefense* — **Lacking funds, Army cuts back on spending.** Army Vice Chief of Staff General Richard Cody directed the Army last week to stop ordering many spare parts and supplies in an effort to pare back spending until Congress passes the fiscal year 2006 emergency supplemental spending bill to fund operations in Iraq and Afghanistan. “Although we anticipate that Congress will finish the bill in June, we need to take action now to control spending in the Operation and Maintenance, Army (OMA) appropriation and stay within the law,” according to a Wednesday, May 26, memo issued by Cody. “This measured response will provide appropriate controls on our spending of OMA resources and will minimize the impact to our mission,” Cody writes. The memo lays out how the Army will begin to cut spending on a week−to−week basis through the month of June.
Source: http://www.military.com/features/0,15240,99145,00.html

[Return to top]

Banking and Finance Sector

7. *May 31, Associated Press* — **Hackers gain access to server hosting bank Websites.** Premier Banks of Minnesota says there is no evidence so far that hackers stole and used consumer data when they diverted customers from Premier's Website to a phony site that asked for customers' credit card and ATM personal−identification numbers. President Mark Novitski said the Website was immediately shut down. Premier Banks, which operates 22 branches, was among more than 100 banks across the nation that were affected when hackers gained access to a server operated by Goldleaf Technologies Inc., on Thursday, May 25. Goldleaf is host to Websites mostly for smaller community banks. Goldleaf spokesperson Scott Meyerhoff said the security breach affected about 150 to 175 bank Websites for anywhere from a minute to an hour and a half. Premier Banks notified the FBI and Federal Deposit Insurance Corp. and plans to send letters to its customers about the incident, advising them to change their online passwords, Novitski said.
Source: http://www.thestate.com/mld/thestate/business/14703801.htm

8. *May 30, 9 News (CO)* — **Colorado Governor signs identity theft bill into law.** Colorado has joined 48 other states nationwide in criminalizing identity theft. Governor Bill Owens signed into law Tuesday, May 30, House Bill 1326 which makes identity theft a Class 4 felony,

punishable by up to six years in prison per victim. Now, Vermont is the only state in the country that does not have a specific crime of identity theft. "There's no question identity theft is a growing problem in Colorado," said Owens, who cited Federal Trade Commission statistics showing Colorado ranking fifth highest among states nationwide in the number of identity theft victims per capita. Owens also signed House Bill 1347 into law which establishes the Identity Theft and Financial Fraud Board within the Department of Public Safety. The Board will help local police officers investigate and district attorneys prosecute cases of identity theft.
Source: http://www.9news.com/acm_news.aspx?OSGNAME=KUSA&IKOBJECTID=87427b53−0abe−421a−0012−402a04886ba9&TEMPLATEID=0c76dce6−ac1f−02d8−0047−c589c01ca7bf

9. *May 30, Sweetwater Reporter (TX)* — **Scam alert in Texas.** The Sweetwater, TX Police Department is warning residents about a current scam to steal bank account information. An official−looking letter claims the recipient has won the “El Gordo Spanish Sweepstake Lottery/International Promotions Program.” The recipient is asked to supply information, including the name, date of birth, identification number (Social Security number), and bank account information so they can identify the winner and deposit the winnings. The scam is distributed via a “confidential” and professional−looking form which the recipient is asked to fill out and fax to the company with a copy of identification.
Source: http://www.sweetwaterreporter.com/articles/2006/05/30/news/n ews2.txt

10. *May 29, Consumer Affairs* — **Scam targets job hunters on Careerbuilder.com.** According to the office of Illinois Attorney General Lisa Madigan and government offices in other states, scam artists have contacted job hunters through CareerBuilder.com regarding a bogus "Donations Handler" position with an international housing charity. The message claimed the charity was located in Norway and described the organization as similar to Habitat for Humanity. The Donations Handler's responsibility is to accept donation checks, deposit them into a personal bank account, and then send payment to the charity. Individuals who accepted the bogus position received cashiers' checks sent in the mail from Atlanta, GA. The victims were to deposit the cashiers' checks into their personal bank accounts and wait until funds were made available, then withdraw a portion and send it via Western Union to a Ukrainian account. By the time the victim had withdrawn funds from their accounts and sent them to the fake charity account, they realized the cashiers' checks were fraudulent. The victims reported losing between $500 and $2,000. The scammers have used different charity names, including: Abantehome.org, Adeonahome.org, Adriahome.org, Alenahome.org, Alstedehome.org, Amalia Int'l, Amaliahome.org, Concordia, DWIO.org, DIO, PWHome, and Public Wish.
Source: http://www.consumeraffairs.com/news04/2006/05/career_buildin g_scam.html

11. *May 26, Websense Security Labs* — **Phishing Alert: Standard Chartered Bank (Hong Kong).** Websense Security Labs has received reports of a new phishing attack that targets customers of Standard Chartered Bank, Hong Kong. Users are lured to a fraudulent Website with a spoofed e−mail message. Once they have arrived at the fraudulent site, any login attempts cause users to be prompted for their personal banking information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =497

12. *May 26, ABC 7 (TX)* — **ID theft hits home for railroad employees.** On the heels of the Veteran's Administration admission that a disk containing social security numbers and dates of

birth for up to 26.5 million veterans was stolen, Union Pacific (UP) Railroad officials say a similar thing has happened to them. The ABC−7 I−Team has learned that a computer holding social security numbers and birth dates on approximately 30,000 UP employees has been stolen from the home of a UP employee in Omaha, NE. UP officials sent a letter to employees warning them of the potential for identity theft due to the security breach. The letter also states that like the Veteran's Administration, a UP employee failed to follow company security procedures, leading to the accidental disclosure of sensitive information.
Source: http://www.kvia.com/global/story.asp?s=4956113

[Return to top]

Transportation and Border Security Sector

13. *May 31, Associated Press* — **Three hurt as plane makes emergency landing at Dulles.** A United spokesperson says United Express flight 7512 landed at Dulles International Airport just after 8:30 p.m. EDT on Tuesday, May 30, while its landing gear on the nose of the plane was still up. The flight was headed to Dulles from Houston, TX. Fifty−six passengers and four crewmembers were on board at the time, and the passengers were evacuated while on the runway. Washington Airports Authority spokesperson Tara Hamilton says three people were taken to local hospitals. Their injuries were believed to be minor.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=49831

14. *May 31, CNNMoney* — **Delta pilots approve latest pay cuts.** Pilots at Delta Air Lines ratified a new round of concessions, according to the union. The vote was 61 percent in favor and 39 percent opposed to the tentative agreement, reached April 14, which will save the airline $280 million annually. Pilots will be paid 14 percent less than they were before the airline's September bankruptcy filing. The ratification probably ends the threat of a crippling strike at the nation's No. 2 air carrier, which analysts had warned could have led to the permanent closure of the Atlanta−based airline. That in turn could have caused a crisis for airline passengers, who are already looking at airlines filling an unprecedented high percentage of available seats during the summer travel season, even with Delta staying in operation. The airline issued a statement praising the vote, saying it is making progress in its efforts to emerge from bankruptcy.
Source: http://biz.yahoo.com/cnnm/060531/053106_delta_pilots.html?.v =2

15. *May 31, Toledo Blade (OH)* — **General cargo booming at Ohio port, but dredging concerns grow.** General cargo business at the Port of Toledo continues to boom, more than tripling during the start of this year’s Great Lakes shipping season. But it’s a boom that the port director says is at risk because of inadequate channel dredging by the U.S. Army Corps of Engineers. “Dredging has been a real concern since I got here, and it has not been alleviated,” said Warren McCrimmon, seaport director for the Toledo−Lucas County Port Authority for nearly four years. So far, McCrimmon said, a reported dredging backlog of between three million and four million cubic yards of sediment in the Maumee River and Maumee Bay shipping channels has not created the same degree of trouble that the Great Lakes Maritime Task Force, a coalition of lakes shipping interests, is reporting in other ports, including Cleveland and Lorain. At 25 miles, the dredged channel leading into Toledo’s port is one of the longest on the Great Lakes. The Maumee Bay portion is intended to be 28 feet deep and 500 feet wide.

Source: http://toledoblade.com/apps/pbcs.dll/article?AID=/20060531/NEWS11/60531046/−1/NEWS

16. *May 31, Herald News (NJ)* — **Airspace proposal comment extended.** The Federal Aviation Administration (FAA) has extended the public comment period for its airspace redesign plans from June 1 to July 1. The FAA, which is looking to expand jet routes over the Northeast to get more planes in the sky, moved the deadline on Tuesday, May 30, after receiving "numerous" complaints from residents and local officials, said spokesperson Jim Peters. The Port Authority of New York and New Jersey, which operates the region's three major airports and Teterboro Airport, also opposes the proposals and plans to submit its written comments by the end of the week. FAA officials, meanwhile, welcomed the opportunity for more time to respond to concerns about plans that, they believe, would reduce delays and untangle the Northeast's complicated network of flight routes.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2OTQxOTI5JnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5Mg==

17. *May 31, Associated Press* — **United Express flight overruns runway in central Wisconsin.** A United Express flight overran the runway on a landing at Central Wisconsin Airport Tuesday, May 30, according to the airport manager. The 44 passengers and three crewmembers were not injured, said manager Tony Yaron. Investigators from the National Transportation Safety Board were investigating Wednesday, May 31. The CRJ 200 regional jet was coming from Chicago and tried to land on the north−south runway at the two−runway airport. It came to rest in a grassy area about 200 yards north of the runway. The flight, United Flight 6979, was operated for United by SkyWest Airlines out of Utah.
Source: http://www.journaltimes.com/articles/2006/05/31/ap−state−wi/ d8huro981.txt

18. *May 31, Reuters* — **U.S. tightens security on New England−Canada border.** The United States has tightened security with Canada in its northeast corner to the dismay of businesses and residents accustomed to crossing the world's longest undefended border with little more than a wave of a hand or a flash of a driver's license. Since last week, most travelers from Canada are being required to show identification and submit to background checks at U.S. border posts in Vermont, New Hampshire, and Maine, said Ted Woo, U.S. Customs and Border Protection spokesperson in Boston. Porous in vast stretches and often invisible, America's 5,500−mile border with Canada is drawing closer scrutiny after President Bush, Mexican President Vicente Fox, and Canadian Prime Minister Stephen Harper agreed in March to work together on border security. While Washington focuses on illegal immigration on the volatile U.S. southern border, a sophisticated drug−smuggling tunnel discovered last year between Vancouver and Seattle and the 1999 arrest of the "millennium bomber" on Canada's western border highlight concerns about the northern boundary.
Source: http://abcnews.go.com/US/wireStory?id=2024603

19. *May 31, Associated Press* — **Passenger service remains disrupted by freight train accident.** Some Amtrak passenger service between Albany and Syracuse remains disrupted because of a freight train derailment in the Mohawk Valley. Amtrak officials say the company is busing passengers on two eastbound and two westbound trains around the accident site, located just west of Amsterdam, NY, in Montgomery County about 35 miles northwest of Albany. Two

other trains operating between Albany and Niagara Falls have been canceled. More than a dozen cars on a CSX freight train went off the tracks on Tuesday, May 30. The cars were empty but contained traces of ethanol, prompting local emergency officials to evacuate residents of the hamlet of Tribes Hill.
Source: http://www.wcax.com/Global/story.asp?S=4970467&nav=4QcS

20. *May 30, TheStreet* — **Southwest's artful approach.** A partnership with ATA Airlines, forged in a 2004 deal to acquire gates at Chicago's Midway Airport, is providing Southwest Airlines with options it never had before. Through a code−share agreement, Southwest can put its passengers on ATA flights to congested airports like New York's LaGuardia, Dallas−Fort Worth International and Washington's Reagan National, on over−water flights to Hawaii and, potentially, on international flights, as well. Privately held ATA gets something too: passengers. Already, about 25 percent of all ATA bookings result from the Southwest relationship The deal is good business for both airlines. Southwest says its code−share revenue, derived from tickets that involve connections between the two airlines, was $50 million in 2005. Each carrier gets the revenue for flights on its aircraft. When passengers use the Southwest site to book ATA−only flights, ATA pays Southwest a fee for that service. Code−shares allow airlines to sell tickets on one another's flights. ATA does things that can't be easily integrated into the Southwest model of quick turnaround times, high utilization of a Boeing 737 fleet and domestic−only flying, says Joseph Loew, a senior vice president at ATA.
Source: http://www.thestreet.com/_googlen/stocks/transportation/1028 8680.html

21. *May 30, Transportation Security Administration* — **Private screening contract for Greater Rochester International Airport.** The Transportation Security Administration (TSA) on Tuesday, May 30, announced a private screening contractor for New York's Greater Rochester International Airport under the Screening Partnership Program (SPP). TSA awarded the contract for security screening services for passenger checkpoint and checked baggage operations from vendors that submitted proposals and are among the 34 private business screening companies identified on TSA's Qualified Vendor's List. The total contract award value, including options, is approximately $46 million. Under SPP, the Federal Security Director for Greater Rochester and Elmira−Corning Regional airports will remain responsible for overseeing TSA security standards and managing contractor performance.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01e89f7

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

22. *May 31, Rapid City Journal (SD)* — **Atypical strain of bovine spongiform encephalopathy found in U.S. cattle.** The two cases of bovine spongiform encephalopathy (BSE) found in U.S. cattle over the past year came from a rare strain of BSE found largely in Europe that scientists

are only beginning to identify, according to research by a French scientist. Researchers in France and Italy who presented their work at an international conference in England reported two rare strains of BSE that are harder to detect and affect mainly older cattle. Thierry Baron of the French Food Safety Agency presented research indicating that a 12−year−old Texas cow testing positive for BSE last June, and the 10−year−old Alabama cow that tested positive in March, showed identical testing patterns to a small number of BSE cases in France, Sweden and Poland. Animal scientists are calling such strains "atypical" BSE, which is different from the "typical" BSE caused by cattle eating feed with ruminant offal contaminated with a BSE protein. They don't know whether the atypical strains are caused by something else or simply appear spontaneously in older, susceptible cattle.
Source: http://www.rapidcityjournal.com/articles/2006/05/31/news/loc al/news05.txt

23. *May 31, Associated Press* — **Foot−and−mouth disease found in cattle in China.** At least 10 cattle in central and western China have been sickened by foot−and−mouth disease but the outbreaks have been brought under control, the Agriculture Ministry said. Last week, seven cattle fell sick in Changyang County in Hubei province and another three were infected in Jiayuguan in the western Gansu province, the ministry said in a statement on Tuesday, May 30. The state laboratory for foot−and−mouth disease control confirmed the outbreaks of the Asia 1 type of the illness on Monday, May 29, the ministry said.
Source: http://www.cattlenetwork.com/content.asp?contentid=40986

[Return to top]

Food Sector

24. *May 31, USAgNet* — **Korea sets dates of U.S. beef imports.** South Korea said it will begin importing beef from approved beef processing plants in the U.S. on June 7. South Korea inspectors examined food−safety procedures at U.S. beef packing and slaughtering facilities in May. South Korea closed its market to U.S. beef in December 2003 after the U.S. confirmed its first case of bovine spongiform encephalopathy. As with other countries that have resumed U.S. beef imports, South Korea set certain conditions on the types of beef that can be imported. South Korea will only allow beef from cattle younger than 30 months of age. In addition, U.S. processors must remove specified risk material −− primarily the brain and spinal cord −− from the carcass. Also, only boneless beef can be imported. In 2003, South Korea imported approximately 200,000 metric tons of U.S. beef.
Source: http://www.usagnet.com/story−national.cfm?Id=1025&yr=2006

[Return to top]

Water Sector

25. *May 25, U.S. Geological Survey* — **Report shows where arsenic is most likely in New England's ground water.** Many private ground−water wells in New Hampshire and Maine may have arsenic at concentrations close to or above federal safety standards for public water supplies. A recently released study by the U.S. Geological Survey (USGS) shows the likely locations of elevated arsenic. Bedrock aquifer wells −− often known as rock, deep, or artesian

wells −− are the most common type of well installed for homes in the region and it is the bedrock aquifer that is the primary source of arsenic in the locations where it is elevated, according to the findings. The study identifies factors that may contribute to high arsenic in wells, and confirms findings from previous studies. Private wells supply drinking water for over 40 percent of the population of northern New England (20 percent of all of New England) and are not regulated by state and Federal agencies. The study concluded that geology was the most significant factor related to arsenic in wells. Other factors include the chemistry of the ground water and characteristics of local aquifers. Modeling the Probability of Arsenic in Groundwater in New England as a Tool for Exposure Assessment:
http://nh.water.usgs.gov/Publications/2006/es051972f.pdf
Source: http://www.usgs.gov/newsroom/article.asp?ID=1513

[Return to top]

Public Health Sector

26. *June 01, Australian* — **Bird flu outbreaks may be hidden.** Indonesia and China could be downplaying their outbreaks of bird flu, the United Nations (UN) warned. The UN's World Organization for Animal Health (OIE) and Food and Agriculture Organization (FAO) said some countries were under−reporting cases of the deadly bird flu H5N1 amid growing concern of a pandemic. Outbreaks in China, Indonesia and African countries could be worse than their governments were reporting. "We know that some countries might be under−reporting ... most do not do it deliberately," the coordinator of the OIE's bird flu taskforce, Christianne Bruschke, said. "We are concerned about China and Indonesia because the virus seems to be so widespread that we could not get all the information. It is difficult to know about each individual outbreak in a back yard." FAO chief veterinary officer Joseph Domenech said under−reporting of avian flu was "not most of the time deliberate". In parts of Africa, he said, it could take a month or two just to send a sample from an infected bird to a laboratory for testing. The World Health Organization has warned that it had only a three−week window to stamp out any local outbreaks of bird flu in humans through mass vaccinations and quarantine.
Source: http://www.theaustralian.news.com.au/story/0,20867,19324098− 2702,00.html

27. *May 31, Reuters* — **Indonesian boy tests positive for bird flu.** A 15−year−old Indonesian boy has tested positive for the H5N1 bird flu, a senior health ministry official said on Wednesday, May 31, citing results of a local laboratory. The boy, from Tasikmalaya town in west Java, was admitted to hospital on May 29 and died a day later. Government officials who visited the boy's village found that he had contact with infected poultry near his home and his own chickens died two weeks ago. The boy's grandfather was a chicken farmer and 40 of his chickens died recently.
Source: http://today.reuters.com/news/newsArticle.aspx?type=scienceNews&storyID=2006−05−31T080708Z_01_HKG211838_RTRUKOC_0_US−BIRDFLU−INDONESIA.xml&archived=False

28. *May 30, Reuters* — **Significant increase in diabetes prevalence in U.S.** More than one out of every three individuals in the U.S. have diabetes and another 26 percent have impaired fasting glucose, which increases the risk of developing diabetes, new study findings suggest. The prevalence of diagnosed diabetes has increased in recent years, while undiagnosed diabetes and

impaired fasting glucose has remained constant over the past decade. The findings are based on an analysis of four years of data from the National Health and Nutrition Examination Survey (NHANES). The study included information on 4,761 adults, age 20 years or older, who were classified according to their glycemic status. Over 35 percent of study participants, representing 73.3 million individuals had diabetes or impaired fasting glucose in 2002. A total 9.3 percent had diabetes in 1988−2002 and the prevalence of undiagnosed remained stable at 2.8 percent during this period. However, the prevalence of diagnosed diabetes rose from 5.1 percent in 1988−1994 to 6.5 percent in 1999−2002. They also estimate that about one third of diabetics are undiagnosed.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−05−30T224217Z_01_ARM081731_RTRIDST_0_HEALTH−SIGNIFICANT−DIABETES−PREVALENCE−DC.XML&archived=False

29. *May 30, Agence France−Presse* — **Scientists meet to discuss bird flu.** Scientists from some 100 countries began a two−day conference in Rome, Italy, to try to define the exact role of migratory birds in the spread of avian flu, one of several mysteries puzzling researchers nearly three years after the first outbreaks. Some 300 experts on bird flu are meeting Tuesday, May 30, and Wednesday, May 31, at the headquarters of the Food and Agriculture Organization. Scientists are puzzled over why some species of wild aquatic birds are more efficient carriers of the disease than others. The most efficient prevention of a human pandemic is still based on the control of the disease at source in domestic birds.
Source: http://news.yahoo.com/s/afp/20060530/hl_afp/healthbirdfluunfao_060530182624;_ylt=AttWYA5EgdYmWXQHh1rzErCJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *May 31, Department of Homeland Security* — **DHS announces $1.7 billion in homeland security grants.** The U.S. Department of Homeland Security (DHS) announced Wednesday, May 31, the recipients of $1.7 billion in fiscal year 2006 Homeland Security Grant Program (HSGP) awards. The grants will enhance the ability of states, urban areas, and territories to prepare for and respond to terrorist attacks and other disasters. In fiscal year 2006, DHS adopted a risk and effectiveness−based approach to allocating funding for certain programs within HSGP. This approach aligns federal resources with national priorities and targets capabilities established by the Interim National Preparedness Goal to generate the highest return on investment in increasing the nation's level of preparedness. HSGP funds can be used for planning, organization, equipment, training, exercises, management, and administration costs.
FY 2006 HSGP Allocations: http://www.dhs.gov/interweb/assetlibrary/grants_st−local_fy0

6.pdf
Source: http://www.dhs.gov/dhspublic/display?content=5666

31. *May 31, Department of Homeland Security* — **DHS and animal groups encourage Americans to include their pets when preparing for emergencies.** The U.S. Department of Homeland Security (DHS) announced Wednesday, May 31, a joint effort with the American Kennel Club, the American Society for the Prevention of Cruelty to Animals, American Veterinary Medical Association, and the Humane Society to encourage pet owners to prepare for emergencies. The Department's Ready Campaign and these animal health and welfare organizations developed a new brochure that highlights the key steps pet owners should take to prepare themselves and their animals. The new brochure suggests making a pet emergency supply kit including food, water, medicines and medical records, collar with ID tag, a leash or harness, and a picture of the pet with its owner. It also recommends having an emergency plan and learning which shelters in their area or along their evacuation route will allow pets in the event of an emergency.
Brochure: http://www.ready.gov/america/_downloads/pets.pdf
Source: http://www.dhs.gov/dhspublic/display?content=5665

32. *May 30, U.S. Department of Defense* — **New Defense Logistics Agency initiatives improve DoD's hurricane, disaster response.** With hurricane season just days away, three new initiatives have officials at the Defense Logistics Agency (DLA) headquarters confident they're more prepared than ever to support the Federal Emergency Management Agency (FEMA). One outcome of a series of meetings DLA had with FEMA is a new interagency agreement between the Department of Defense (DoD) and FEMA that streamlines the pre−planning and disaster assistance process. The agreement, signed March 31, helps clear up any misunderstandings about responsibilities and authorities when a disaster occurs. The new agreement gives DLA responsibility for procuring, storing and managing materiel for disaster relief missions, along with the required funding. Two new additional DLA initiatives will help ensure the agency can respond faster and more efficiently. In 2005, DLA kept track of the goods it provided FEMA but lost sight of where they went after the handoff. For the upcoming hurricane season, a new in−transit visibility system will use satellites to track DLA deliveries to the disaster zone. In addition, a new deployable depot capability will also help improve the way relief supplies are distributed. Once established, the depot would be able to support 200,000 people a day with meals, water ice, tarps and other supplies.
Source: http://www.defenselink.mil/news/May2006/20060530_5291.html

33. *May 30, New York Times* — **As hurricane season looms, states aim to scare.** Convinced that tough tactics are needed, officials in hurricane−prone states are trumpeting dire warnings about the storm season that starts on Thursday, June 1, preaching self−reliance and prodding the public to prepare early and well. Cities are circulating storm−preparation checklists, counties are holding hurricane expositions at shopping malls and states are dangling carrots like free home inspections and tax−free storm supplies in hopes of conquering complacency. But the main strategy, it seems, is to scare the multitudes of people who emergency officials say remain blasé even after last year's record−breaking storm season. To persuade residents to heed evacuation orders, the Florida Division of Emergency Management is broadcasting public service announcements with recordings of 911 calls placed during Hurricane Ivan in 2004. Speaking of the tactics, Craig Fugate, Florida's emergency management director, said, "We're

going to use a sledgehammer." This save−yourselves approach comes after government agencies were overwhelmed by pleas for help after last year's storms and strongly criticized as not responding swiftly or thoroughly enough to the public need. Now, officials have said repeatedly, only the elderly, the poor and the disabled should count on the government to help them escape a hurricane or endure its immediate aftermath.
Source: http://www.nytimes.com/2006/05/31/us/31prepare.html?hp&ex=1149134400&en=891fee11a14932d7&ei=5094&partner=homepage

[Return to top]

Information Technology and Telecommunications Sector

34. *May 31, VNUNet* — **DigiKeyGen pornographic spyware guilty of blackmail.** Security experts issued a warning Wednesday, May 31, about a newly intercepted spyware program called DigiKeyGen. When users run DigiKeyGen, they receive passwords that supposedly allow them access to pornographic Websites. At the same time, a spyware program and an alleged anti−spyware application are installed on the computer without the user's knowledge. It then warns the unwitting user that their computers are infected and offers them an anti−spyware program to clean the system for $49.95.
Source: http://www.vnunet.com/vnunet/news/2157203/digikeygen−porn−wo rm−guilty

35. *May 30, Security Focus* — **Mozilla Firefox Marquee denial−of−service vulnerability.** Mozilla Firefox is prone to a denial−of−service vulnerability when parsing certain HTML content. Analysis: Successfully exploiting this issue allows attackers to consume excessive CPU resources in affected browsers, denying service to legitimate users.
Vulnerable: Mozilla Firefox 1.5.3.
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18165/references

36. *May 30, Security Focus* — **Kaspersky Anti−Virus unspecified denial−of−service vulnerability.** Kaspersky Anti−Virus is prone to a denial−of−service vulnerability. Analysis: This is due to a failure in the application to handle unspecified files. Attackers could cause the application to consume excessive CPU and memory resources, resulting in a denial−of−service.
Vulnerable: Kaspersky Labs Kaspersky Anti−Virus for Linux Servers 5.5; Kaspersky Labs Kaspersky Anti−Virus for Linux Servers 5.0.5.
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/16942/references

37. *May 30, Security Focus* — **Multiple Mozilla products IFRAME JavaScript execution vulnerability.** Multiple Mozilla products are prone to a script execution vulnerability. Analysis: The vulnerability presents itself when an attacker supplies a specially crafted e−mail to a user containing malicious script code in an IFRAME and the user tries to reply to the mail. Arbitrary JavaScript can be executed even if the user has disabled JavaScript execution in the client.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/16770/info
Solution: Mozilla has released an advisory, along with fixes to address this issue. For more information: http://www.securityfocus.com/bid/16770/references

Source: http://www.securityfocus.com/bid/16770/discuss

38. *May 30, Sophos* — **Trojan broadcasts bogus spyware warning to networked users.** Sophos has discovered a new twist in the tactics used by malware to promote controversial anti−spyware products. After infecting a computer, the Troj/Paymite−J Trojan horse looks for other computers on the network and sends a fake warning message to them claiming that they are infected by spyware. "Because the warning message displays the computer's IP address, some may think it contains greater legitimacy than a regular pop−up advert. Furthermore, because the message's recipient has not run any suspicious code on their computer they may not realize it has been sent from a PC belonging to one of their colleagues on the network," said Graham Cluley, senior technology consultant at Sophos. Refer to the source to see a screen shot of the fake warning message.
Source: http://www.sophos.com/pressoffice/news/articles/2006/05/paym itej.html

39. *May 30, Tech Web* — **Trojan horse BeastPWS−C: The second Trojan to pose as Microsoft patch.** A second Trojan posing as a Microsoft patch or update has been reported, security firms said Tuesday, May 30. According to Sophos, the Trojan horse "BeastPWS−C" starts with a spoofed e−mail from Microsoft that claims a new vulnerability in the WinLogon Service is out and about. WinLogon is the log−in service for Windows NT, 2000, and XP. The spammed message includes a link to a purported patch. Users who click on the URL actually download the Trojan, not a patch. BeastPWS−C, said Sophos, logs keystrokes and sends them to a hacker's e−mail account. The other Trojan, dubbed "Sinowal.u" by Kaspersky Labs, is German−language spam that claims to be from Microsoft Windows Update, but is actually a Trojan contained within the file attachment.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=188501301

40. *May 30, IDG News Service* — **StarOffice hit by its first virus.** The first virus affecting StarOffice was detected Tuesday, May 30. The virus, named "Stardust," uses macros to attack the office suite from Sun Microsystems. Since the virus has not yet been launched with malicious intent, a teenager hacker may have written it, said Roel Schouwenberg, senior research engineer for Kaspersky Lab. If a user opens a document infected with Stardust, every StarOffice text document, with a ".sxw" extension, or document template, with a ".stw" extension, will be infected. When one of those documents is launched, it opens an adult image hosted on a tripod.com server.
Source: http://www.infoworld.com/article/06/05/30/78762_HNstaroffice virus_1.html?source=rss&url=http://www.infoworld.com/article /06/05/30/78762_HNstarofficevirus_1.html

41. *May 30, Pensacola News Journal (FL)* — **Florida Chamber of Commerce offering free e−mail protection during hurricane season.** The Florida Chamber of Commerce will make a free emergency e−mail protection service available to all Florida businesses during the 2006 hurricane season. The free service, called Digital Disaster Preparedness, is designed to protect and preserve e−mail traffic if businesses' IT infrastructures are vulnerable to hurricane−related damage.
The service can be requested online: http://www.appriver.com/hurricane2006/
Florida Chamber of Commerce:
http://www.floridachamber.com/flcchw/hw.dll?page&t=homepage& file=home

Source: http://www.pensacolanewsjournal.com/apps/pbcs.dll/article?AID=/20060530/BUSINESS/605300311

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT continues to receive reports of data theft that targets online users and Federal government web sites. Recently, Veteran Affairs data was stolen from the home computer system of a Veterans Affairs (VA) employee. This data contained large amounts of personally identifiable information, such as, names, social security numbers, and dates of birth. Over 26 million veterans and some spouses are affected by this incident. The VA is continuing to investigate this issue and working to inform affected parties of this incident so that the appropriate steps can be taken to protect against this information being misused. US−CERT recommends that users take the following measures to protect against data theft:

Encrypt sensitive data on your local hard drive and back up mediums.

Attend Security Awareness training to gain a better understanding of your organization's policies and procedures for handling sensitive data.

Restrict access to sensitive data from Internet connected systems.

For additional information, please review the following URL:
http://www.first.gov/veteransinfo

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is currently researching a zero day vulnerability in Microsoft Word. US−CERT and Microsoft will continue to investigate the public reports to help provide additional guidance as necessary. There is currently no patch available for this vulnerability. For more information please review the following:

Cyber Security Tip: http://www.us−cert.gov/cas/tips/ST04−010.html

Microsoft Security Advisory (919637):
http://www.microsoft.com/technet/security/advisory/919637.ms pxEAF

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 6588 (AnalogX), 135 (epmap), 25 (smtp), 54856 (−−−), 80 (www), 32788 (−−−), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer